

## **Supporting Statement for the Reporting and Disclosure Requirements Associated with Regulation P (unnum Reg P; OMB No. 7100-0294)**

### **Summary**

The Board of Governors of the Federal Reserve System, under delegated authority from the Office of Management and Budget (OMB), proposes to extend for three years, without revision, the reporting and disclosure requirements in connection with Regulation P, which implements the Protection of Nonpublic Personal Information provisions of the Gramm-Leach-Bliley Act of 1999 (GLBA).<sup>1</sup> The PRA classifies a regulation that imposes reporting, recordkeeping, or disclosure obligations required by a regulation as an “information collection.”<sup>2</sup> The PRA requires the Federal Reserve to renew authority for an information collection every three years. On April 9, 2003, a notice of the renewal was published in the *Federal Register* for public comment.<sup>3</sup>

The information collection pursuant to Regulation P is triggered by the establishment of a relationship between a customer and a financial institution. The regulation ensures that financial institutions provide customers notice of the privacy policies and practices of financial institutions and a means to prevent the disclosure of nonpublic personal information, in certain circumstances. Where applicable, financial institutions are required to provide an initial notice and an annual notice of their privacy policies and practices, opt-out notices, and revised notices containing changes in policies and procedures.

Under the PRA, an agency must estimate the burden of a regulation on its own “respondents” (institutions it supervises that are subject to the regulation). Thus, the Federal Reserve accounts for the paperwork burden associated with Regulation P for the 9,500 financial institutions supervised by the Federal Reserve that must comply with the regulation.<sup>4</sup> The Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), National Credit Union Administration (NCUA), Federal Trade Commission (FTC), and Securities and Exchange Commission (SEC) (“the agencies,” also including the Federal Reserve) are responsible for estimating the burden of their equivalent privacy regulations on their respondents. Nevertheless, the agencies jointly agreed on burden estimates when they promulgated the privacy regulations in 2000. An inter-agency working group of PRA

---

<sup>1</sup> The Protection of Nonpublic Personal Information provisions are codified at 15 U.S.C. § 6801 *et seq.* Regulation P is located at 12 CFR Part 216.

<sup>2</sup> 44 U.S.C. § 3501 *et seq.*

<sup>3</sup> The collection of information under Regulation P is assigned OMB No. 7100-0294 for purposes of the PRA.

<sup>4</sup> Section 216.3(q) of Regulation P defines Federal Reserve regulated financial institutions as: State member banks, subsidiaries of state member banks, bank holding companies and its subsidiaries or affiliates, branches and agencies of foreign banks, commercial lending companies owned or controlled by foreign banks, and corporations operating under section 25 or 25A of the Federal Reserve Act.

staff (“inter-agency PRA staff”)<sup>5</sup> has been jointly reviewing and revising those burden estimates. To avoid expiration of the authority for the information collection while the review is ongoing, the Federal Reserve will publish for comment burden estimates based on assumptions used in 2000, and then publish revised final estimates once the inter-agency PRA staff has finalized them. Under this approach, the Federal Reserve would publish for comment an estimate of 427,500 hours for the collective annual burden imposed by Regulation P on the 9,500 respondents. (See the Respondent Burden section for more detail)

## **Background and Justification**

The GLBA (Sec. 504), Public Law No. 106-102 directed the agencies to issue regulations to implement notice requirements and restrictions on a financial institution’s ability to disclose nonpublic personal information about consumers to nonaffiliated third parties.

A financial institution’s precise responsibilities under GLBA and the privacy regulations depend on whether it is dealing with a “consumer” or a “customer.” A consumer is an individual who obtains a financial product or service from a financial institution that is primarily for personal, family, or household purposes; a customer is a consumer who has an ongoing relationship with a financial institution. A financial institution must provide notice to its customers about its privacy policies and practices and may not disclose nonpublic personal information about any consumer (whether or not a “customer”) to nonaffiliated third parties unless (1) the consumer has not elected to opt out of the information sharing after receiving required disclosures or (2) the disclosure is permitted under one of the regulation’s exceptions. A financial institution must also provide an annual privacy notice to its customers but does not have to provide the notice to consumers who are not customers.

## **Description of Information Collection**

Subpart A of the regulation prescribes the required disclosures for privacy and opt-out notices. The opt-out provisions of the regulation enable consumers to prevent a financial institution from disclosing nonpublic personal information to third parties that are not affiliated with the financial institution. The provisions do not restrict the disclosure of nonpublic personal information among affiliated companies nor do they restrict the disclosure of information about businesses or corporations.

### **Privacy and opt-out notices (Subpart A)**

Regulation P imposes four disclosure requirements on financial institutions: initial privacy notice, annual privacy notice, revised privacy notice (notice of change in terms), and opt-out notice. In addition, the regulation imposes two reporting requirements on consumers: an initial notice that the consumer opts out (if the consumer so chooses), and

---

<sup>5</sup> The staffs are from the Federal Reserve, FDIC, OCC, and OTS.

a notice to the institution during the course of the relationship if the consumer elects to change his or her opt-out status.

### *Financial Institutions' Disclosure Requirements*

**Initial privacy notice to consumers.** Generally, a financial institution must provide consumers a clear and conspicuous notice that accurately reflects its privacy policies and practices. An institution must have provided the initial privacy notice to all current customers as of the regulation's mandatory effective date of July 1, 2001. After that date, a financial institution must provide the initial privacy notice to all new customers when they commence the customer relationship. A financial institution is not required to provide an initial notice to a consumer if it does not have a customer relationship with the consumer and it does not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by the regulation. To reduce burden, the regulation authorizes simplified and short forms of the initial privacy notice for use under certain conditions.

**Annual privacy notice to customers.** Financial institutions must provide to customers a clear and conspicuous notice that accurately reflects an institution's privacy policies and practices not less than once in a twelve-month period during the continuation of the customer relationship.

*Information to be included in privacy notices.* The initial notice and annual notice each must include all of the following items of information:

- the categories of nonpublic personal information about the consumers that the institution collects;
- the categories of nonpublic personal information about the consumers that the institution discloses;
- the categories of affiliates and nonaffiliated third parties to whom the institution discloses nonpublic personal information about the consumers, other than those parties excepted under the regulation;
- the categories of nonpublic personal information about former consumers that the institution discloses and the categories of affiliates and nonaffiliated third parties to whom the institution discloses nonpublic personal information about former consumers, other than those parties excepted under the regulation;
- if an institution discloses nonpublic personal information to service providers or joint marketers, a description of the categories of information the institution discloses and the categories of third parties with whom the institution has contracted;
- an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right;
- any disclosures regarding the ability to opt out of disclosures of information among affiliates;

- the institutions' policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and
- description of nonaffiliated third parties subject to exceptions under the regulation.

**Revised privacy notice (notice of change in terms).** Certain changes to a financial institution's privacy policies or practices trigger a requirement to provide consumers a revised notice that accurately describes the institution's current policies and practices. After an institution has made certain changes to its disclosure practices, it may not directly or through affiliates disclose a new category of nonpublic personal information about a consumer to a new category of entity before giving the consumer (1) a new notice that accurately describes the policies and practices, (2) a new opt-out notice, and (3) a reasonable opportunity to opt out.

**Notice of right to opt out.** Depending on a financial institution's information-sharing practices, it must provide an opt-out notice at the start of a consumer relationship. An opt-out notice may also be required when the institution issues a revised privacy notice.

### *Consumers' Reporting Requirements*

**Consumer's notice of invocation of opt out right.** To invoke his or her right to opt out, a consumer must notify the institution. The consumer must be given a reasonable opportunity to opt out before information may be shared outside of the permitted exceptions.

**Consumer's continuing right to opt out.** A consumer has the right to change or update his or her opt-out status with an institution at any time during his or her continued relationship with the institution. The financial institution must comply with the consumer's direction as soon as reasonably practicable, and the consumer's direction to opt-out under the regulation is effective until revoked by the consumer. If a customer relationship terminates, the customer's opt-out direction continues to apply to the nonpublic personal information that the financial institution collected during or related to the relationship. If the individual subsequently establishes a new customer relationship with the institution, the opt-out direction that applied to the former relationship does not apply to the new relationship.

To facilitate compliance with these requirements, Regulation P gives examples of "nonpublic personal information," "consumer," "consumer reporting agency," "customer" and "personally identifiable financial information" among other things. The regulation also provides guidance on the timing of notices to customers and the means by which consumers can exercise their opt-out rights. Appendix A of the regulation contains sample clauses to aid financial institutions in developing disclosure notices.

## **Time Schedule for Information Collection**

The disclosure requirements of Regulation P are relationship-specific and must be provided within the time periods established by law and regulation as discussed above. The regulation also contains consumer reporting requirements. A consumer must be allowed a reasonable opportunity to opt out before otherwise permitted information sharing may occur. A consumer has the right to change or update the consumer's opt-out status with the institution at any time during a continued relationship.

## **Legal Status**

In connection with the promulgation of Regulation P in 2000, the Board's Legal Division determined that the consumer reporting requirements and financial institution disclosure requirements associated with the regulation are authorized by the Federal Reserve Act (12 U.S.C § 248) and the GLBA (Pub. L. 106-102, Sec. 504). Since the Federal Reserve does not collect any information, no issue of confidentiality normally arises.

## **Estimate of Respondent Burden**

In early 2003, inter-agency PRA staff agreed to jointly re-estimate the paperwork burden of their privacy regulations. To avoid missing PRA renewal deadlines, however, they agreed meanwhile to separately publish for comment estimates based on the 2000 assumptions; the last comment period (that of the Federal Reserve) would be followed by a joint final notice in the *Federal Register* using revised estimates. Pursuant to this understanding, OCC, FDIC, and OTS have published initial *Federal Register* notices using the 2000 estimates; the comment periods have closed.

Using the 2000 assumptions, the Federal Reserve estimates 427,500 hours for the collective annual burden imposed by Regulation P on the 9,500 respondents for which the Federal Reserve is responsible to estimate paperwork burden. This figure would represent 7 percent of the total Federal Reserve System paperwork burden

In 2000, the agencies agreed to use their total number of institutions as the total number of respondents for both the institutions' disclosure requirements and the consumers' reporting requirements. In the absence of any information about how much time institutions and consumers would spend annually complying with the regulation, the agencies estimated a response time of 40 hours (approximately one business week) for creating and distributing the required initial notice, and one hour for each of the five other requirements. As indicated above, inter-agency PRA staff will likely recommend increasing the hourly estimate of the per-disclosure burden while decreasing the estimate of the number of respondents for at least some of the six requirements.

---

	<i>Number of respondents</i>	<i>Estimated annual frequency</i>	<i>Estimated response time</i>	<i>Estimated annual burden hours</i>
<u><i>Disclosure requirements</i></u>				
Initial notice	9,500	1	40 hours	380,000
Annual notice	9,500	1	1 hour	9,500
Opt out notice	9,500	1	1 hour	9,500
Notice of change in terms	9,500	1	1 hour	9,500
<u><i>Consumer reporting requirements</i></u>				
Opt out notice	9,500	1	1 hour	9,500
Continuing right to opt out	9,500	1	1 hour	9,500
<i>Total</i>				427,500

---

Based on a rate of \$20 per hour, the estimated cost to the public for this information collection is \$8,550,000.

### **Consultation Outside of the Agency**

As mentioned above, the Federal Reserve is consulting with the FDIC, OCC, and OTS about revising the estimate of the paperwork burden.

### **Sensitive Questions**

This collection of information contains no questions of a sensitive nature, as defined by OMB guidelines.

### **Estimate of Cost to the Federal Reserve System**

Since the Federal Reserve does not collect any information, the cost to the Federal Reserve System is negligible.